Data Managers Interest Group
Institute of Clinical and Translational Research

April 17, 2012
Privacy & Security Contacts

- [hipaa@jhmi.edu](mailto:hipaa@jhmi.edu)
- [network.security@jhmi.edu](mailto:network.security@jhmi.edu)
- IT Help Desk – 410.735.4357
- Or you can call me
  - Darren Lacey – Chief Information Security Officer
    - [dll@jhu.edu](mailto:dll@jhu.edu)
    - 410.735.4477
Let’s start with some numbers
**HIPAA Breaches >500 since 2009**

<table>
<thead>
<tr>
<th>Breach Types</th>
<th>Number</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking/IT Incident</td>
<td>44</td>
<td>14</td>
</tr>
<tr>
<td>Improper Disposal (Paper)</td>
<td>73</td>
<td>23</td>
</tr>
<tr>
<td>Lost /Stolen Computer/Server</td>
<td>41</td>
<td>13</td>
</tr>
<tr>
<td>Lost/stolen media or portable electronic devices</td>
<td>47</td>
<td>15</td>
</tr>
<tr>
<td>Lost/Stolen Laptops</td>
<td>77</td>
<td>25</td>
</tr>
<tr>
<td>Unauthorized access</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>Email</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Other</td>
<td>18</td>
<td>6</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>314</td>
<td>100</td>
</tr>
</tbody>
</table>

Ways to think about the numbers

• Hacking incidents make up slightly more than half of large incidents related to higher education
• Across all industries hacking makes up ¼ of incidents
• There are many more incidents related unauthorized access but these involve fewer than 500 patients
HITECH Act Changes in HIPAA

• Notification required for any breach not just SSN or financial information
• Increased fines and penalties
• 150 audits annually of covered entities starting next year
• Meaningful use requires security risk assessment
Things the HIPAA Cops Hate

• WEP – Wireless networks
• Unencrypted email and insecure transmissions
• Lack of monitoring of business associates
• Failure to monitor unauthorized access to patient records
• Lack of accurate inventory of devices, applications and services
• Inadequate training and awareness
Risk areas at Hopkins

- Application complexity
- Disclosure and use accounting
- Downstream data sets
- Personally owned devices
- Collaborative multi-site projects
- Kudzu-like web presence
- Network proximity to defense-oriented research
What can researchers do?
Encrypt your laptop, including the one you bring from home!!!

It’s cheap, usually easy
Laptop Encryption Options

• Mac’s
  – Lion: use FileVault2, whole disk encryption
  – Pre-Lion: use FileVault or TrueCrypt folder encryption

• Windows XP – Checkpoint encryption through Hopkins (often pre-installed) or TrueCrypt FDE

• Windows7 – (Enterprise or Ultimate) MS Bitlocker or TrueCrypt FDE
Do you have a project Web site?

No, good.

Yes, prepare to do some work and lots of maintenance
Web Security Threats

- Check your server for sensitive files
- Database access controls and monitoring
- Watch your forms and URL’s for potential attacks
  - SQL Injection
  - Cross-site scripting
- Validate all input
- Test your error screens
- Monitor any platform vulnerabilities (e.g. PHP)
- Sound server management practices
Write up a short data management and sharing plan

For data security and quality. Think of it as version control
Parts of the plan

- Documented data extractions
- De-identification and anonymization
- Downstream data use agreements
- Dynamic access control lists
- Data sharing approaches – lowest common denominator
- Disposal and life cycle management
Tools you can use

• Jshare for file sharing (internal and external)
• Sharepoint for internal file sharing and version control (don’t recommend large PHI datasets)
• Winzip/7zip – encrypted folders
• JIRA – for collaboration, but it should be authenticated through SM (don’t recommend large PHI datasets)
General security controls

• Access control for administrative access
• Log management and monitoring of servers
• Symantec or Forefront Endpoint protection
• Be circumspect about cloud services – but these are improving rapidly
• Policies against insecure storage –
  – USB’s not only get stolen but are malware magnets
  – Home machines are generally not to be trusted